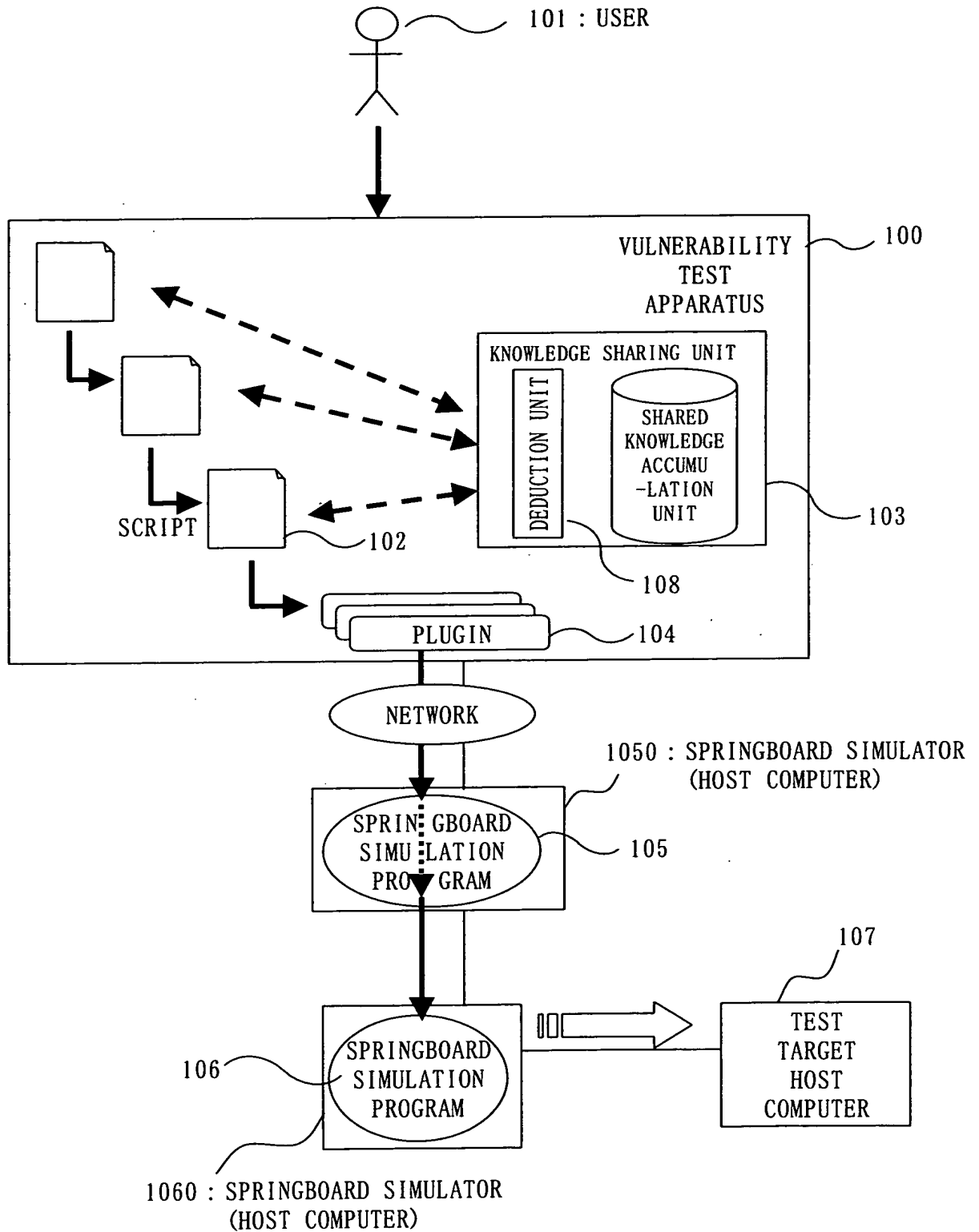
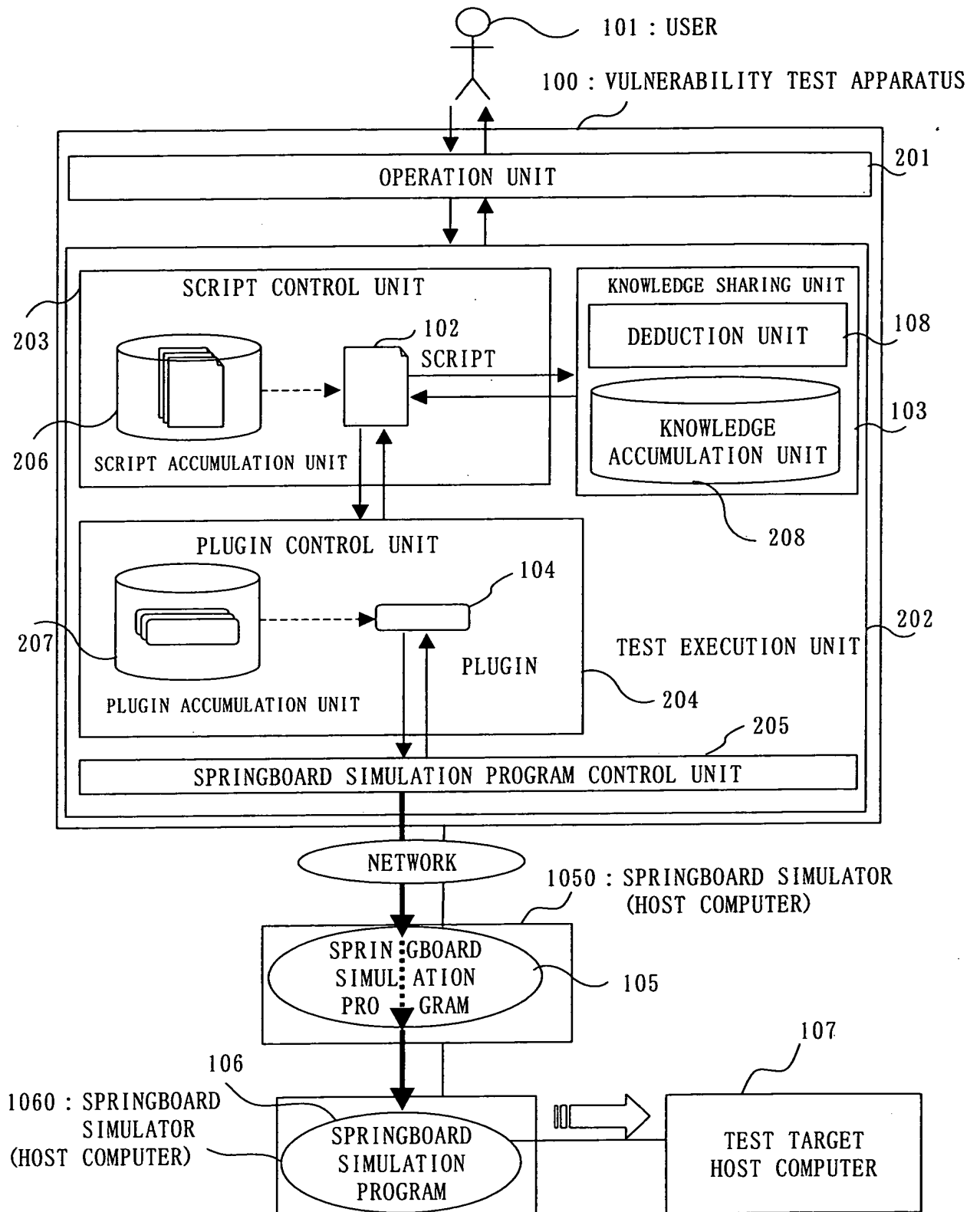


1/9
Fig. 1

2/9
Fig. 2

3/9

Fig. 3

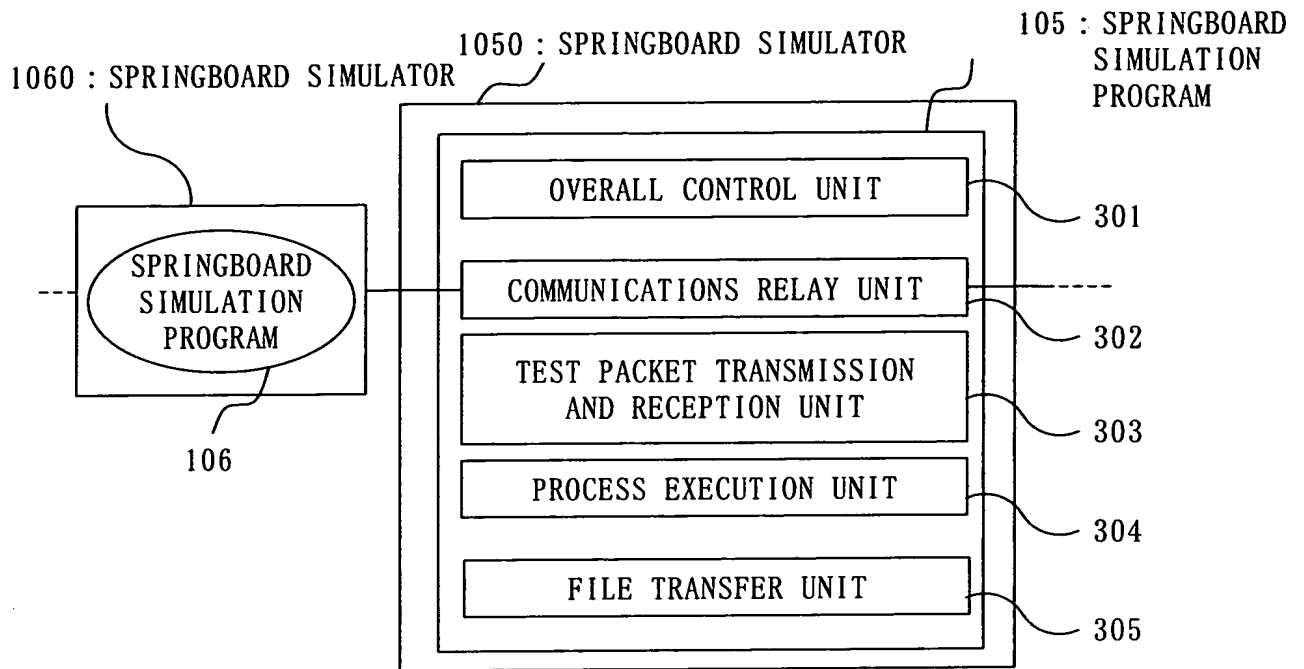
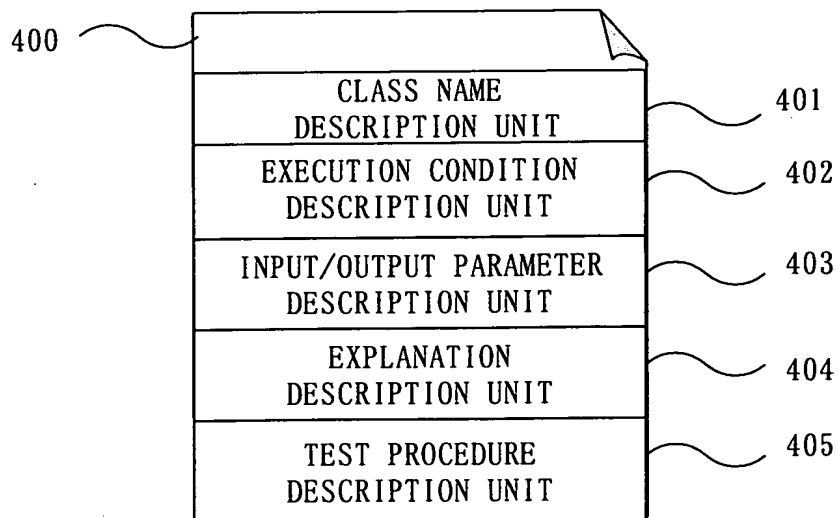
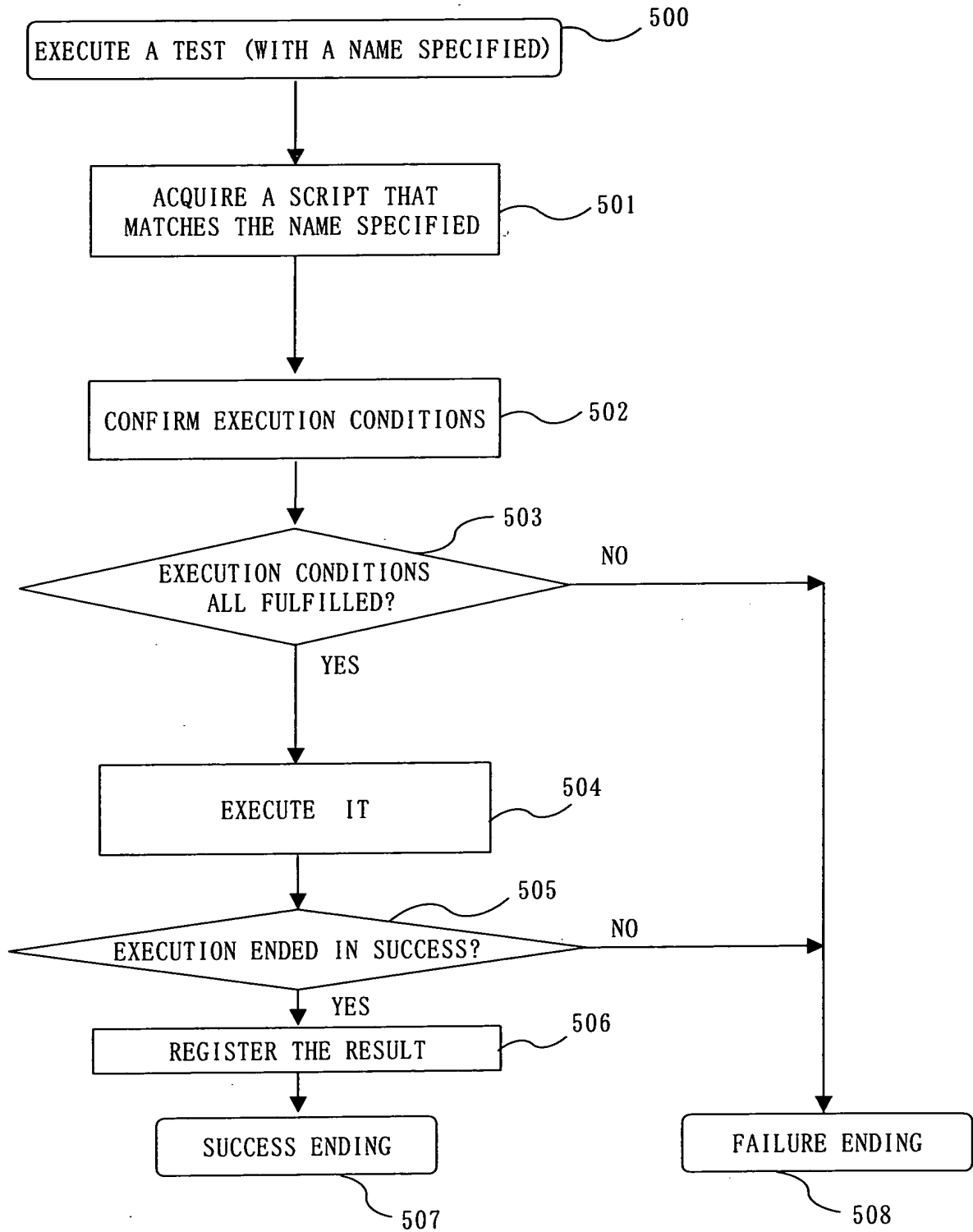
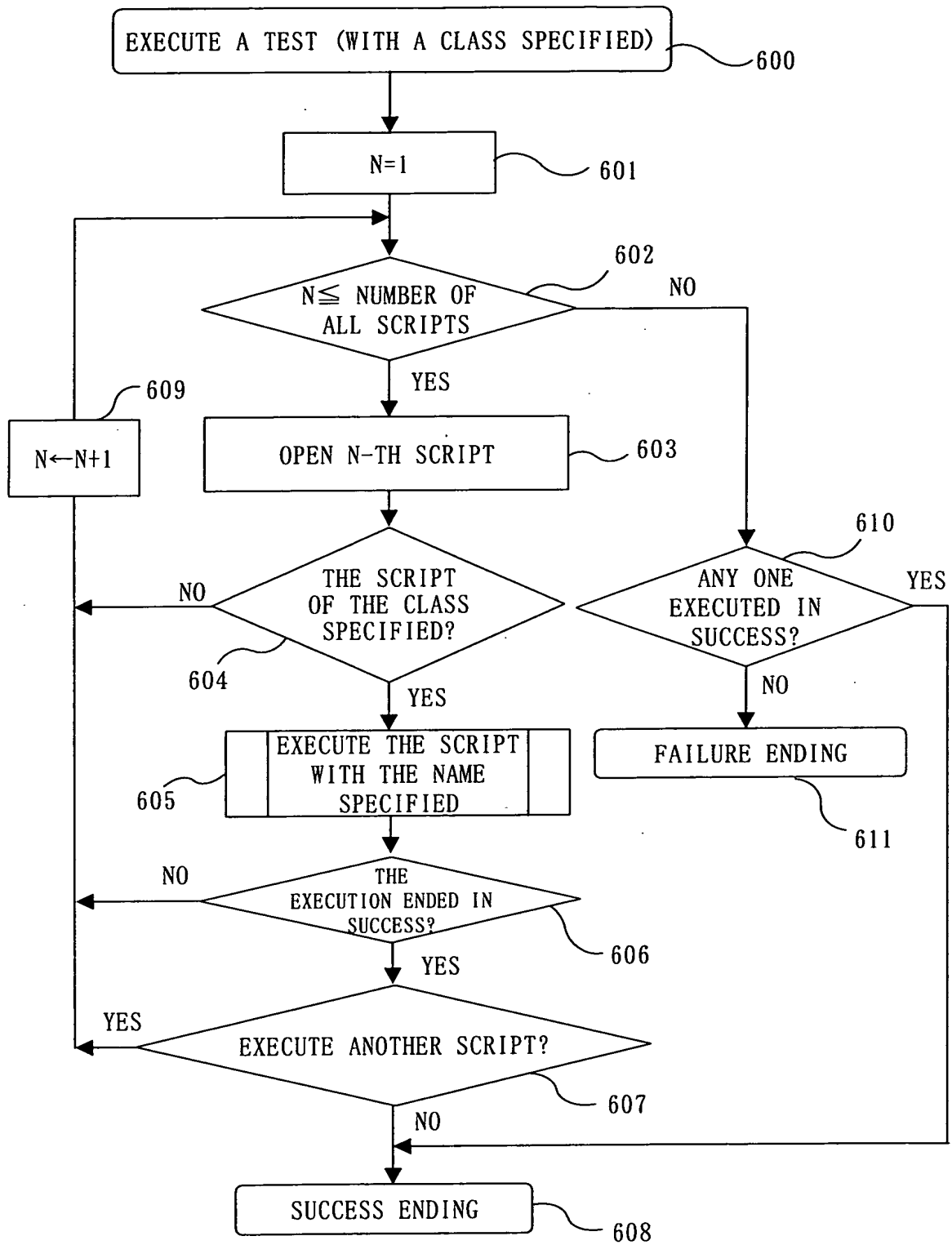


Fig. 4



4/9
Fig. 5

5/9
Fig. 6

6/9

Fig. 7

```
admin( HOST, 'root' ) :-
    os( HOST, 'UNIX' );

admin( HOST, 'administrator' ) :-
    os( HOST, 'WINDOWS' ).

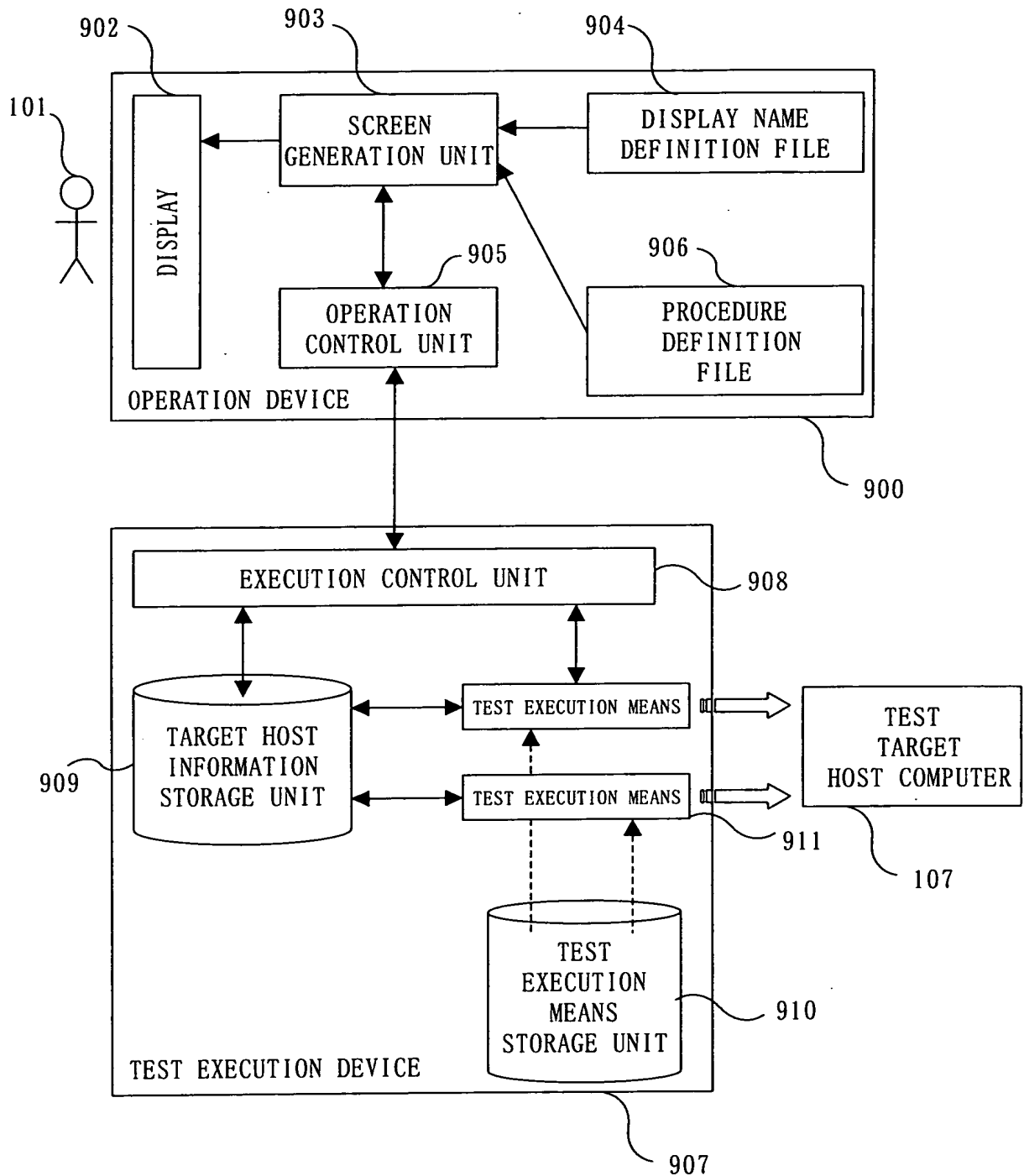
web( HOST, PORT ) :-
    script( 'find_web_port', [ HOST ], [ PORTS ] ),
    member( PORT, PORTS ).

cgi( HOST, PORT, CGINAME ) :-
    script( 'check_cgi', [ HOST, PORT, CGINAME ], _ ).
```

Fig. 8

```
# -----BEGIN_SCRIPT_PROPERTY-----
#Class:      command_exec
#Pre-condition:  web( HOST, PORT ), cgi( HOST, PORT, "phf" )
#Input:      HOST      string  "TEST TARGET HOST ADDRESS"
#Input:      CMD       string  "COMMAND SEQUENCE TO BE EXECUTED"
#Output:     RESULT    string  "OUTPUT THE COMMAND EXECUTION"
#Description: "THE COMMAND IS EXECUTED USING PHF."
#-----END_SCRIPT_PROPERTY-----

Perl BASED EXECUTABLE CODE. . .
```

7/9
Fig. 9

8/9
Fig. 10

```
#  
# PROCEDURE DEFINITION FILE.  
#  
  
# PROPERTY NAME  
# PLUGIN_TYPE  
  
#  
# SYNTAX:  CATEGORY_KEY' = ' CATEGORY_DISPLAY_NAME(' ¥ EXEC_TYPE) (' ¥ CATEGORY_DESCRIPTION)  
#          EXEC_TYPE = 0(ne)/A(11)/Q(very)  
  
PORTSCAN=PORT SCAN Q TO SCAN A PORT ATTACKABLE ON THE TARGET HOST.  
  
GET_FILE=FILE ACQUISITION 0 TO ACQUIRE A FILE SPECIFIED FROM THE TARGET.  
  
PASSWORD_CRACK=PASSWORD CRACK Q TO EXTRACT AN ACCOUNT AND A PASSWORD FROM A PASSWORD FILE  
SPECIFIED.
```


Fig. 11

